

Contents

Preface — V

Acknowledgment — IX

Notation — XI

Sets, relations, and functions — **XI**

Landau symbols — **XII**

1 Algebraic structures — 1

1.1 Numbers — **1**

1.2 From semigroups to vector spaces — **2**

1.3 Basic group theory — **6**

1.4 A glimpse into rings — **10**

1.4.1 Matrix rings — **10**

1.4.2 Polynomials — **11**

1.4.3 Ideals and quotient rings — **12**

1.4.4 Complex numbers — **13**

2 Elementary number theory — 15

2.1 Modular arithmetic — **15**

2.2 Euclidean algorithm — **17**

2.3 Fundamental theorem of arithmetic — **18**

2.4 Bits and bytes — **19**

2.5 Error detection for article numbers — **20**

2.6 Chinese remaindering — **21**

2.7 Fermat's primality test — **24**

2.8 Fast exponentiation — **25**

2.9 RSA encryption — **27**

2.10 Euler's totient function — **29**

2.11 Finite multiplicative subgroups of fields — **31**

2.12 Fibonacci numbers — **33**

2.13 Recursion depth of the Euclidean algorithm — **37**

Exercises — **38**

Summary — **41**

3 Some useful growth estimates — 42

3.1 Factorials — **42**

3.2 Binomial coefficients — **43**

3.3 Least common multiple — **46**

3.4 Prime number density — **49**

3.5	Bertrand's postulate — 51
	Exercises — 53
	Summary — 55
4	Discrete probability — 56
4.1	Probabilities and expected values — 56
4.2	Jensen's inequality — 60
4.3	Birthday paradox — 61
	Exercises — 62
	Summary — 64
5	Combinatorics — 65
5.1	Enumerative combinatorics — 65
5.2	Binomial coefficients — 67
5.3	Average case analysis of bubble sort — 78
5.4	Inclusion and exclusion — 79
5.5	Rencontres numbers — 82
5.6	Stirling numbers — 83
5.6.1	Stirling numbers of the second kind — 84
5.6.2	Stirling numbers of the first kind — 88
5.7	Bell numbers — 92
5.8	Partition numbers — 93
5.9	Catalan numbers — 96
5.10	Dyck words — 96
5.11	Binary trees — 98
5.12	Expected height of binary search trees — 100
	Exercises — 102
	Summary — 106
6	Generating functions — 108
6.1	Ordinary generating functions — 108
6.2	Fibonacci numbers — 109
6.3	Catalan numbers — 110
6.4	Stirling numbers of the second kind — 111
6.5	Partition numbers — 111
6.6	Growth of the partition numbers — 115
6.7	Pentagonal number theorem — 117
6.8	Exponential generating functions — 120
6.9	Stirling numbers of the first kind — 121
6.10	Bell numbers — 122
	Exercises — 123
	Summary — 125

7 Group actions and special families of groups — 126

- 7.1 Group actions — 126
- 7.2 Orbit-stabilizer theorem — 127
- 7.3 p -groups — 128
- 7.4 Cyclic groups — 129
- 7.5 Dihedral groups — 130
- 7.6 Symmetric groups — 131
- 7.7 Alternating groups — 134
- 7.8 Nilpotent groups — 138
- 7.9 Unit triangular groups — 139
- Exercises — 142
- Summary — 143

8 Graph theory — 144

- 8.1 Basic terms — 144
- 8.2 Eulerian and Hamiltonian cycles — 150
- 8.3 Trees — 152
- 8.4 Cayley's formula — 154
- 8.5 Hall's marriage theorem — 156
- 8.6 Stable marriage — 158
- 8.7 Menger's theorem — 160
- 8.8 Maximum flows — 161
- 8.9 Max-flow min-cut theorem — 162
- 8.10 Dinic's algorithm — 167
- 8.11 Planar graphs — 170
- 8.12 Euler's formula — 172
- 8.13 Colorings of planar graphs — 174
- 8.14 Planar separators — 174
- 8.15 Ramsey's theorem — 177
- Exercises — 181
- Summary — 184

9 Order structures and lattices — 185

- 9.1 Partial orders — 185
- 9.2 Complete partial orders — 189
- 9.3 Denotational semantics — 190
- 9.4 Least fixed points of monotone mappings — 193
- 9.5 Lattices — 195
- 9.6 Complete lattices — 197
- 9.7 Modular and distributive lattices — 198
- 9.8 Boolean lattices — 203
- 9.9 Boolean rings — 204

XVIII — Contents

9.10	Stone's general representation theorem —	207
	Exercises —	210
	Summary —	211

10 Boolean functions and circuits — 212

10.1	Shannon's upper bound —	214
10.2	Shannon's lower bound —	215
10.3	Lupanov's asymptotically optimal upper bound —	217

Solutions — 221

Chapter 2 —	221
Chapter 3 —	225
Chapter 4 —	228
Chapter 5 —	231
Chapter 6 —	237
Chapter 7 —	240
Chapter 8 —	242
Chapter 9 —	248

Bibliography — 251

Index — 253